MSPC RESPONSE TO PRIVACY WORKING GROUP'S REQUEST FOR INFORMATION

April 7, 2025

INTRODUCTION

The Main Street Privacy Coalition (MSPC)[1] appreciates the opportunity to submit these comments in response to the House Energy and Commerce Committee's Privacy Working Group (PWG) following its Request for Information (RFI).

The MSPC's trade-association members represent a broad array of companies that line America's Main Streets, including retailers, restaurants, grocery and convenience stores, hotels, resorts and hospitality companies, gas stations, and a wide range of franchise establishments. Our members' companies interact with consumers on a daily basis and can be found in every town, city, and state, providing jobs, supporting our economy, and serving Americans as a vital part of their communities. Collectively, the industry sectors that MSPC member trades represent directly employ approximately 34 million Americans and contribute $4.5 trillion to the U.S. gross domestic product.

Privacy laws apply to, and must work for, Main Street businesses that directly serve Americans in their daily lives. MSPC recommends privacy legislation embrace the core principles we have developed since 2019 to ensure a balanced and effective national privacy framework. These principles can be found in *Appendix A (attached)* and on our website.[2] Each has important implications for federal privacy legislation, and our considerations in formulating them from our business and legislative experience are discussed in our responses to the RFI's specific questions on the following pages.

[continued]

[1] Additional information about the Main Street Privacy Coalition (MSPC) is available at: https://mainstreetprivacy.com
[2] MSPC's set of principles for federal data privacy legislation are available at: https://mainstreetprivacy.com/principles/

RESPONSES TO OUTLINED RFI QUESTIONS

I. Roles and Responsibilities

Main Street businesses will bear the full burden of regulatory obligations under proposed federal privacy bills. Previous bills have significantly narrowed the obligations of other entities, largely exempting telecom, cable, and big tech service providers from the same obligations to protect consumer privacy as Main Street businesses. We strongly recommend federal privacy law apply *equivalent* data privacy obligations to all businesses.

A. Accounting for Different Roles Among a Wide Range of Business Models

Use Standardized Terms and Definitions: We suggest defining the entities to be covered under federal law using the globally accepted and well-understood definitions of "controller" and "processor" in nearly all comprehensive state privacy laws.[3] By contrast, terms like "business," "covered entity," and "service provider" are more ambiguous terms in their scope and applicability, and should be refrained from use as they have often obscured a clear delineation of roles and responsibilities.

Common Branding and Joint Liability Concerns: An issue that the Committee resolved in its past privacy legislation is the significant negative consequence of holding franchisors and franchisees liable for each other's privacy law compliance. Many franchisees and franchisors share "common branding" (e.g., the franchisees all use the same brand on their restaurant, fitness center, hair salon, etc.) but are distinct companies and should be treated as such. In the past, privacy legislation had initially defined these entities as one single "covered entity" because the businesses operate with "common branding." We appreciated the Committee's prior efforts to remove the "common branding" language from its privacy legislation and we recommend using definitions that avoid making broad groups of independent businesses jointly liable for one another's behavior when there is lack of control.[4]

---

[3] In the substantive provisions of proposed legislation, the PWG should recognize that many so-called "controllers" are small businesses while many "processors" are large, nationwide or global businesses; controllers in this context must be understood as not truly capable of controlling the activities of these processors, who typically use non-negotiable standard-form contracts they draft for the services they provide to collectively millions of SMEs.

[4] The PWG should also recall that, last year, Congress approved a Congressional Review Act action overturning the National Labor Relations Board's joint employer standard. Lawmakers opposed the NLRB rule as it would have incorrectly classified two entities as joint employers *where an entity lacked substantial direct and immediate control over the essential terms and conditions of employment of another entity's employees*. The measure garnered near-unanimous support from House and Senate Republicans, and it is crucial that federal privacy legislation also maintain the vital distinction between separate entities. See roll call votes at: https://clerk.house.gov/Votes/202410 and

B. Appropriate Obligations for Each Role

Delineate the Obligations for Each Role Based on Successful State Law Approach: The vast majority of enacted state laws have delineated the precise obligations of controllers and processors, among other entities, as well as the obligations processors have with respect to controllers.[5] We support the obligations for service providers in state privacy laws in Colorado and Connecticut, which can be summarized as shown in the chart in *Appendix B (attached)*, although we believe all processors should also have equivalent data security requirements to controllers.

Hold Businesses Accountable for Their Own Actions. Each business is in the best position to control its own actions and compliance.[6] A law that relies on controllers having responsibility for the compliance of large nationwide processors will accomplish little, other than adding unnecessary cost and undeserved liability to many Main Street businesses that are not in a position to absorb either.

Direct Statutory Obligations and Equivalent Enforcement for Processors. There were serious flaws with previous privacy bills considered by the Committee that failed to place direct statutory obligations on service providers (i.e., processors) and third parties, and did not subject those businesses to the same enforcement mechanisms as covered entities (i.e., controllers) to ensure their compliance. Last year, H.R. 8818, the American Privacy Rights Act (APRA) removed both direct statutory obligations and enforcement mechanisms for "service providers" (i.e., processors) and third parties in ways that obviated their obligations to protect the consumer data received from "covered entities" (i.e., controllers). As a result, nationwide and global service providers would not have had equivalent privacy obligations or enforcement provisions that applied to even the smallest Main Street businesses, leaving consumers much less protected when processors and third parties handled their personal data.

Balancing Controller/Processor Duties in Responding to Consumers' Privacy Rights Requests: We also urge the PWG to ensure greater balance in the obligations among controllers, processors, and third parties with respect to the processing of

https://www.senate.gov/legislative/LIS/roll_call_votes/vote1182/vote_118_2_00122.htm#position) Similarly, franchises—most of whom are small businesses—within a franchise system operate under the franchisor's trademark but are *distinct entities with no control* over any aspect of their fellow franchisees' business.

[5] These delineations are typically found in state privacy laws' sections with a heading for "roles" and "responsibilities."

[6] This is particularly true for most controllers, which are overwhelmingly small businesses, and their inability to control the actions and compliance of processors, which tend to be large, nationwide businesses.

consumers' privacy rights requests, particularly where small businesses and large nationwide or global service providers are handling the same customers' data and have vastly different contractual bargaining power. All companies handling the chain of personal data should be required to honor consumers' privacy rights requests. Congress should not rely on private contracts alone to create legal obligations between parties, particularly between businesses that vary greatly in size and bargaining power.

A federal privacy framework should have controllers act as the recipient of consumer privacy rights requests and require controllers to pass valid requests onto processors who are necessary to fulfill such requests. Controllers' responsibilities from there should be limited to doing what they themselves can do to comply with such requests, plus communicating what the processors must do with their obligations to fulfill such requests.[7] Controllers should not be required to police compliance by those processors nor should controllers be liable for processors' failures to comply with consumers' rights requests.[8]

C. Accounting for Size and Accompanying Protections, Exclusions, or Obligations

Prohibit Liability-Shifting of Statutory Obligations Via Contractual Provisions. Privacy responsibilities should not simply be shifted from one industry sector onto another. It is manifestly unfair to businesses that bear the brunt of those shifted burdens when it should be the other businesses' own obligations to the consumer. Too often powerful businesses within the telecom, cable, and tech industry sectors use their superior market power to shift what should be their own responsibilities onto their clients via contractual requirements, leaving Main Street businesses with outsized compliance burdens and costs. If Congress relies on parties' contractual relationships to ensure privacy protections, with such contracts being exalted into having the force of federal law behind them, it will leave holes in consumer privacy rights because federal enforcement agencies will have no effective way to compel service providers or third parties to comply with the law. To avoid this, a federal

[7] The PWG should carefully review the provisions of Senator Moran's *Consumer Data Privacy and Security Act* that was last introduced on April 29, 2021. The Moran bill sets the rights and responsibilities of parties in the law in ways that avoided the pitfalls of more recent privacy legislation considered by the Committee since 2022. In particular, the Moran bill ensured a process for processing consumer rights requests that carefully balanced the obligations among controllers, processors, and third parties to ensure all parties handling the same consumer's data honored their rights requests in an accountable way.

[8] For example, if a controller transmits a valid consumer's data deletion request to a processor, the controller should not be liable for the processor's failure to delete the consumer's data. The liability for that failure should rest with the processor.

privacy framework must create effective federal statutory obligations that hold each party accountable.

Correct Imbalances Among Industry Sectors' Privacy Laws to Meet Consumers' Expectations: We are concerned with exemptions for financial institutions subject to the Gramm Leach Bliley Act (GLBA) from consumer data privacy legislation. GLBA, a law enacted in 1999, is outdated by decades in its extremely narrow data privacy rules, which do not provide anything close to the privacy protections the Committee previously considered extending to all other consumer data.[9] *See Appendix C (attached)*

II. Personal Information, Transparency, and Consumer Rights

Consumers should be empowered to control their personal data used by organizations and, consistent with that, businesses should be permitted to responsibly use such data consumers share with them to better serve their needs. MSPC urges the PWG to consider the strong consensus of state privacy laws in balancing these interests.

Personal Information and Small Business Scoping. Most state privacy laws scope their applicability to small businesses based on the amount of personal information they process in one year. However, for many small businesses that only collect payment card data for the sole purpose of completing a transaction, this can inadvertently create a mechanism whereby a high-volume low-dollar payments transactions by a small business like a restaurant or convenience store may cross the threshold to subject them to all provisions of a privacy law simply because they accepted digital payments. The PWG should review how Connecticut solved for this issue.[10]

Market Segmentation Data. It is important to recognize that market segmentation data is not sensitive. Many products are appropriately marketed based on gender or ethnicity (e.g., apparel, beauty products, food and grocery items, gender-specific hygiene products, etc.). Attributes such as these either should not be included in a definition of sensitive personal information or, if they are included, legislation should permit the continued legitimate use

[9] To illustrate the disparity between today's best practices for privacy and what financial institutions are subject to, we prepared a chart in *Appendix C* comparing the base privacy protections in privacy laws in European Union (EU) and California law to the current narrow regime that applies to the financial services industry through the Gramm Leach Bliley Act ("GLBA"). The chart makes clear that GLBA does not protect data privacy in the way that most consumers (and legislators) have now come to expect. Most Americans would be surprised to learn they have far more privacy protections when buying an ice cream cone than when engaging in sensitive financial transactions involving their life savings with their financial institution.

[10] MSPC urges the PWG to consider the improved language of the Connecticut privacy law, S.B. 6 enacted in 2022 (Public Act No. 22-15), in which Section 2 excludes counting (for determining the applicability of the law to small businesses) any "personal data controlled or processed solely for the purpose of completing a payment transaction."

of such market segmentation data to serve customers as they expect to be served in the offering and promotion of products and services relevant to them.

Web-Browsing Behavior. Some previous legislative proposals have attempted to include within the definition of sensitive data the browsing behavior of individuals online or on mobile applications, which would be highly disruptive for businesses that personalize their websites or apps to meet the consumer's preferences. The proper place to address the concerns with marketing based on browsing behavior is in the provisions creating an opt-out for targeted advertising. The provisions should only apply to data that is collected over time and across unaffiliated websites. Limitations that prevent direct interactions between a business and its own customers are not appropriate for privacy legislation other than through opt-out choices, as found in most state laws.

III. Existing Privacy Frameworks & Protections

Preemption of State Law. MSPC supports federal, preemptive legislation to establish a single, uniform national privacy law. Previous legislation in the Committee did not achieve this goal and would have left American consumers with different rights depending on where they lived. A preemption provision should be crafted to meet the standards the Supreme Court has consistently ruled are sufficient to create a preemptive federal law.[11] The clearest way to do that is through a preemption provision specifying precisely which state laws are preempted and making it clear that future state laws related to the federal law would be similarly preempted.

IV. Data Security

MSPC supports federal privacy and data security laws that ensure all businesses have obligations to provide reasonable data security appropriate to their size, nature of business, and scope of transactions involving personal data in which they engage.

Consumer-facing businesses must comply with breach notification laws in 54 states and U.S. territories. However, many exempt financial institutions and processors from breach notification requirements. Federal privacy law should correct these "breach notice holes" by requiring *all* businesses handling personal data to provide notice to affected individuals of their *own* data security breaches when they occur. This would hold accountable *all* breached entities and create proper incentives to secure data while preventing the shifting of notice obligations onto non-breached businesses.

[11] *See* white paper on Federal Preemption of State Law prepared originally as a memo to the Republican staff of the House Energy and Commerce Committee in 2011 and updated several times, with the most recent edition Feb. 6, 2020.

V. Artificial Intelligence

MSPC recommends artificial intelligence legislation be separate from data privacy legislation. A federal comprehensive data privacy law should ensure that any provisions related to automated decision-making are properly scoped to not be tantamount to a regulation of AI technologies.

VI. Accountability & Enforcement Accountability

Effective enforcement of a federal privacy law requires holding accountable *all* businesses handling consumer data to *equivalent* data privacy standards using the same enforcement mechanisms, thereby creating an even playing field and proper incentives across industry sectors to comply with those standards.

A. Benefits of Exclusive Governmental Entity Enforcement

Every enacted state comprehensive data privacy law relies on *exclusive* government enforcement coupled with a notice-and-cure provision. No comprehensive state privacy laws permit private rights of action to enforce the *privacy* provisions of those laws. Three critical reasons explain why this approach has developed into the appropriate consensus method for ensuring uniform application, interpretation, and enforcement of privacy standards under state privacy laws:

- Meaning of "Reasonable." All comprehensive state privacy laws contain dozens of uses of the words "reasonable" or "reasonably" when setting forth business obligations. Each use raises the possibility of widely different interpretations in meaning. If left to private lawsuits to define what are "reasonable" privacy practices, it would result in endless litigation and differing standards that would call into question practices that government enforcement authorities could find reasonable. It would also chill investment in innovative, responsible new practices to better serve customers in a rapidly evolving environment. Exclusive governmental enforcement is the only way to ensure uniform interpretation and enforcement of the law.[12]

- Robust Compliance with Privacy Laws and Rapid Error Correction. To protect consumers, there must be a mechanism to encourage regulated entities to rapidly get compliance right. All state privacy laws use a notice-and-cure mechanism for this purpose, especially when a law is new. It provides an expedited means for businesses to correct technical errors without fearing

[12] In the Vermont Senate debate on June 17, 2024 (*see* webcast starting at 09:29) over Governor Scott's veto of H. 121, the Vermont Data Privacy Act that included private rights of action, a key argument persuading senators to sustain the veto (i.e., kill the bill) was that the bill had approximately 70 uses of the terms "reasonable" or "reasonably" that could not be left to private litigation in state courts to uniformly interpret and enforce, like the Vermont Attorney General could do and other state AGs did *exclusively* in all other states (except California, which has joint AG and privacy agency authority).

bankrupting lawsuits. The California Attorney General confirmed the benefits of notice-and-cure provisions reporting that 75% of the businesses notified had corrected their errors within 30days.[13] Adversarial litigation takes years and does not lead to timely compliance.

- Private Litigation Disproportionately Impacts Main Street Businesses. Private rights of action have been rejected in the 40% of states that have enacted comprehensive privacy laws because they would disproportionately impact Main Street businesses. Dominant technology companies can force arbitration or otherwise fight litigation. Small Main Street businesses can't. This Committee has seen problems with litigation trolls in many areas of law and passed legislation to stop it.[14] There is a significant risk that a similar cottage industry of *privacy* trolls, if given the chance, would leverage private rights of action against Main Street businesses in bad faith here as well.[15] Finally, as the MSPC raised in its letter opposing private rights of action in the APRA, federal privacy legislation can also disproportionately impact Main Street businesses when exempting other parties from the same type of enforcement.[16]

VII. Additional Information

Preserve Customer Loyalty Rewards and Benefits. A federal data privacy law should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships like loyalty programs. Americans greatly benefit from customer loyalty programs offered by Main Street businesses.[17] State privacy

[13] California Attorney General Bonta reported that, in the first full year of implementing a notice-and-cure provision, 75% of companies notified of potential violations responded by amending their practices to come into compliance within the 30-day cure period, with the remaining 25% either in the process of their 30-day cure period or under further investigation. *See:* https://iapp.org/news/a/california-attorney-general-offer-ccpa-enforcement-update-launches-reporting-tool

[14] To curb the pattern or practice of sending vague and abusive demand letters alleging, in bad faith, patent infringement by Main Street and other businesses, the House Energy and Commerce Committee approved and reported to the House floor H.R. 2045, the *Targeting Rogue and Opaque Letters (TROL) Act*, to protect these businesses from the deceptive acts and practices of patent trolls.

[15] In the previously discussed Vermont Senate vote to sustain the governor's veto of the legislation with private rights of action *(see footnote 12)*, another compelling argument raised in opposition to private rights of action was that Vermont small businesses would be disproportionately impacted by out-of-state trial lawyers, driving up prices for consumers.

[16] The APRA exempted service providers and third parties from almost all enforcement by private rights of action while subjecting all Main Street businesses to this mass litigation threat, creating a severely disproportionate impact on some businesses over other and picking winners and losers in the marketplace.

[17] Bond Brand Loyalty Inc. has issues reports on loyalty programs and benefits to consumers for the past 14 years. In prior years, their reports found that 79% of consumers said loyalty programs make them more likely to continue doing business with the brands offering them and 32% strongly agree a loyalty program makes their brand experience better. The most recent Bond Loyalty Report, released July 25, 2024, found that brands "using loyalty programs well…focused on personalization and superb customer care—both essential aspects of successful loyalty programs. According to the report, participants must be 'recognized' to feel seen, leaning into the human-to-human connections that leave them feeling special." In this report, Bond also reported that the average person participates in 19 different loyalty programs. "The influence of loyalty programs on customer behavior is higher than ever with 79% of consumers being more likely to recommend brands with solid loyalty programs and 85% of consumers saying they are more likely to continue buying from the brand." *See:* https://info.bondbrandloyalty.com/the-loyalty-report-2024-press-release

laws preserve these programs. While we agree that no business should retaliate against a consumer for exercising privacy rights, giving benefits to loyal customers does not retaliate against anyone who doesn't want to participate in those programs. State laws have preserved loyalty plans where consumers voluntarily participate in *bona fide* programs offering better prices and services.[18]

[continued]

[18] These laws use a savings clause clarifying that the non-discrimination provisions shall not be construed to prohibit a business from offering better prices or services in connection with loyalty programs.

Thank you for your consideration of MSPC's views. We would enjoy the opportunity to discuss them with the PWG. Please contact Paul Martino, counsel to MSPC, at pmartino@hunton.com to arrange meetings or request further information.

Respectfully submitted,

American Beverage Licensees
American Hotel & Lodging Association
American Resort Development Association
Direct Selling Association
Energy Marketers of America
FMI, The Food Industry Association
International Franchise Association
National Association of Convenience Stores
National Council of Chain Restaurants
National Grocers Association
National Restaurant Association
National Retail Federation
NATSO, Representing America's Truck Stops and Travel Centers
Retail Industry Leaders Association
SIGMA: America's Leading Fuel Marketers
Small Business & Entrepreneurship Council

Main Street
PRIVACY COALITION

MSPC RESPONSE TO PRIVACY WORKING GROUP'S REQUEST FOR INFORMATION

Appendix A

Main Street Principles for Data Privacy Legislation

American businesses have no higher priority than earning and maintaining trusted relationships with their customers. To preserve those relationships, businesses must protect and responsibly use the personal information that customers share with them. As Congress considers legislative and regulatory solutions to address data privacy concerns, our coalition urges adoption of the following principles.[1]

- **Establish a Uniform National Privacy Law**
  Congress should enact a privacy law that benefits consumers and businesses alike by ensuring *all* personal data is protected in a consistent manner regardless of where a consumer resides.
- **Protect Consumers Comprehensively with Equivalent Standards for All Businesses**
  Federal data privacy frameworks should apply requirements to all industries that handle personal data and should not place a disproportionate burden on certain sectors of the economy while alleviating others from providing equivalent protections of personal data.
- **Create Statutory Obligations (Not Contractual Requirements) for All Entities that Handle Consumers' Data**
  Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts. Service providers and third parties must have statutory privacy obligations when offering data processing, transmission, storage, or other services to collectively millions of Main Street businesses.
- **Preserve Customer Loyalty Rewards and Benefits**
  A federal privacy law should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships such as loyalty programs.
- **Require Transparency and Customer Choice for All Businesses**
  Consumers deserve to know the categories of personal data that *all* businesses collect, how it is generally used to serve them, and the choices they have regarding those uses.
- **Hold Businesses Accountable for their Own Actions**
  Privacy legislation should not include terms that potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of a business partner.
- **Ensure Reasonable Data Security Standards**
  Privacy legislation should include reasonable data security standards for *all* businesses handling consumer data, as well as a uniform rules for *any* businesses suffering a data security breach to notify affected individuals.
- **Establish Effective Accountability and Enforcement**
  Effective enforcement must hold accountable *all* entities handling personal data to *equivalent* data privacy standards using the *same* enforcement mechanisms, thereby creating an even playing field and proper incentives across industry sectors to comply with those standards. Because "mistake-free" compliance is unlikely in this complex area of law, we support the approach adopted in all enacted state privacy laws of coupling *exclusive* governmental entity enforcement with the regulated entity's ability to "cure" non-compliant practices within a limited period of time after timely and specific notice from the governmental authority.

[1] MSPC's principles for federal privacy legislation are also available at: https://mainstreetprivacy.com/principles/

MSPC RESPONSE TO PRIVACY WORKING GROUP'S REQUEST FOR INFORMATION

Appendix B

Comparison of Processor Requirements in Three Key State Privacy Laws that Set the New Standard

- The chart below compares the processor requirements in the three key state privacy laws that were enacted early and set the standard for processor requirements: Virginia, Colorado, and Connecticut. These states passed laws in 2021 and 2022, after California's 2018 California Consumer Privacy Act (CCPA), which *failed to establish* any data processor requirements to protect consumers' data.
- Without statutory processor requirements, small-business controllers would lack the bargaining leverage necessary (in contractual negotiations with much larger data processors) to require processors to ensure the privacy of the controller's customer data when in the processor's hands.
- These key state privacy laws established a strong model that influenced most other state privacy laws, which adopted similar processor requirements to protect consumer data.

✓=Required ☒=Not Required KEY STATES THAT REQUIRED PROCESSORS TO:	VIRGINIA CDPA (2021)	COLORADO CPA (2021)	CONN. SB 6, Sec. 7 (2022)
Ensure Processor's Own Data Security when handling Controller's personal data	☒	✓	☒
Assist Fulfilling Privacy Rights Requests from Individuals and w/ Data Breach Notices	✓	✓	✓
Give Info to Controller to Complete DPAs (Data Privacy Assessments) Required of Controller	✓	✓	✓
Ensure Confidentiality of Personal Data by Processors' Employees w/ Personal Data	✓	✓	✓
Hold Subcontractors to Processor's Terms / Give Controller the Right to Object to Subs	✓ / ☒	✓ / ✓	✓ / ✓
Return/Delete Personal Data at Contract End (at the Choice of the Controller)	✓	✓	✓
Provide Controller Compliance Info Needed to Demonstrate Processor's Legal Compliance	✓	✓	✓
Allow and Cooperate w/ Reasonable Audits or Assessments at the Request of Controller	✓	✓	✓
Respect Cross-Liability Protections (Parties Not Liable for Another Party's Violations of their Own Obligations under the Act)	✓	✓	✓

MSPC RESPONSE TO PRIVACY WORKING GROUP'S REQUEST FOR INFORMATION

Appendix C

Data Privacy Frameworks Adopted by European Union and California, Compared to GLBA Applying to U.S. Financial Institutions

PRIVACY LAW COMPARISON CHART

Consumer Privacy Rights regarding their Personal Information	GDPR (2016)	CCPA (2018)*	GLBA (1999)	Notes
Transparency	✓	✓	!	GLBA: partial transparency; only annually-*mailed* disclosure notice of data uses (w/ some exceptions)
Control (Choices)	✓	✓	✗	GLBA: no meaningful control; opt out *only for* non-affiliate sharing that is not excepted (e.g., some marketing)
Access	✓	✓	✗	
Correction	✓	✓	✗	
Deletion	✓	✓	✗	
Portability	✓	✓	✗	
Breach Notification	✓	!	!	CCPA: CA breach law requires notice, but not CCPA GLBA: Not required (guidance *only* says "should" notify)
Opt-Out of Direct Marketing	✓	✗	✗	GDPR: opt out of processing for direct marketing GLBA: joint marketing agreements override opt-out
Opt-Out of Data Sharing for Targeted Ads	✗	✓	✗	CCPA: opt out of data sharing to third parties for purposes of processing data for targeted advertising
Opt-Out of Data "Sales"	✗	✓	✗	CCPA: opt out of data "sales" to third parties for purposes beyond marketing/advertising (w/ some exceptions)

**CCPA, as amended by CPRA (2020)*